USDA

Privacy Impact Assessment

CRM Common Desktop Application

Revision: 1.3

Natural Resource Conservation Service

Date: October 9, 2009

Document Information

Owner Details	
Name	Kathy Green
Contact Number	970-295-5647
E-mail Address	Kathy.Green@ftc.usda.gov

Revision History			
Revision	Date	Author	Comments
1.0	9 March 2009	Ray Coleman	Initial Draft
1.1	16 March 2009	Kathy Green	Clarification: Description of System
1.2	7 August 2009	Kathy Green	Update owner and clarify system scope
1.3	9 October 2009	Kathy Green	Final approved version for CRM-CD C&A

Distribution List			
Name	Title	Agency/Office	Contact Information

Table of Contents

1 System Information

System Information	
Agency:	Natural Resources Conservation Service
System Name:	NRCS CRM Common Desktop Application
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	The *CRM Common Desktop* system is used for creating, managing, and tracking information for Conservation programs involving grants and easements for a number of programs, including the Wetland Reserve Program (WRP), the Emergency Watershed Protection Program – Flood Plain Easements (EWPP-FPE), and the Farm and Ranch Land Protection Program (FRPP). The system manages funds that have been allocated from the Foundation Financial Information System (FFIS) to state controlled sub accounts.
Who owns this system? (Name, agency, contact information)	Kathy Green, ITC Development Branch Chief, USDA-NRCS, Kathy.Green@ftc.usda.gov, 970-295-5647.
Who is the security contact for this system? (Name, agency, contact information)	Chuck Hart, Information System Security Manager, USDA-NRCS, Chuck.Hart@ftc.usda.gov, (970) 295-5550.
Who completed this document? (Name, agency, contact information)	Ray Coleman, Systems Security Analyst, USDA NRCS Contractor, ray.coleman@ftc.usda.gov, 970-2955-5570.

2 Data Information

2.1 Data Collection

No.	Question	Response

1	Generally describe the data to be used in the system.	**Categories of Data:**
		
		1. **Financial**
		   • Accounting Information Type
		   • Payments Information Type - **(The NRCS *CRM Common Desktop* application does not make payments. All payments are made via the National Finance Center (NFC)).**
		   • Funds Control Information Type
		   • Reporting and Information Information Type
		
		2. **Natural Resources**
		   • Water Resource Management Information Type
		   • Conservation, Marine and Land Management Information Type
		
		3. **General Information**
		   • Refers to Business contact information of customers and partners (i.e., name, phone #, email address)
		
		NOTE: Per NIST SP 800-60 volume II Rev 1, dated November 2007, page 5, the General Information type was added as a catch-all information type. As such, agencies may use this to identify additional information types not defined in the Business Reference Model (BRM) and assign impact levels.
		
		Data being collected by the *CRM Common Desktop* application will be used to process NRCS grants.
		
		• Example: The USDA Natural Resources Conservation Service (NRCS) provides technical and financial support via easements to help landowners with their wetland restoration efforts and purchase development rights to keep productive farms and ranchlands in agricultural uses. This support provides for the restoration of land and/or the purchase of land with the intent of doing restoration.

No.	Question	Response
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☐ Yes ☒ No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No
4	Sources of the data in the system.	• SCIMS DB • NFC- Payment status
4.1	What data is being collected from the customer?	• Public • Financial Additional categorization of information is described in the Security Categorization Document (SCD), located in CoLab.
4.2	What USDA agencies are providing data for use in the system?	• NRCS • NFC • FSA (SCIMS database) NOTE: The *CRM Common Desktop* application will use a web service developed by the Forest Service (FS) to communicate with NFC, but FS is not supplying any data.
4.3	What state and local agencies are providing data for use in the system?	State Conservation Districts
4.4	From what other third party sources is data being collected?	Federal Partners include the agencies listed in question 4.2 above.
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☒ Yes ☐ No – If NO, go to question 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	There is a trusted relationship between the Conservation Districts (CD) and NRCS, which is documented via Memorandum of Understanding. CDs are responsible for ensuring all data is accurate when collected
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Multiple levels of review and approval are required for all critical transactions to ensure Separation of Duties. All financial transactions require a final review and approval from a financial approver.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	The status of financial transactions will be sent back from NFC to NRCS for reconciliation.

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	• Conservation Planning • Conservation Delivery
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.
7.1	What are the other purposes?	
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	☒ Yes ☐ No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☐ Yes ☒ No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☐ No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☐ No
9.3	How will the new data be verified for relevance and accuracy?	
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	• Conservation Planning • Conservation Delivery
11	Will the data be used for any other uses (routine or otherwise)?	☒ Yes ☐ No – If NO, go to question 12.
11.1	What are the other uses?	NRCS must report the status of all payments made to meet Congressional requirements.
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If NO, go to question 13.

No.	Question	Response
12.1	What controls are in place to protect the data and prevent unauthorized access?	The *CRM Common Desktop* application will inherit Access Control from Active Directory and zRoles to implement roles-based access within the application.
13	Are processes being consolidated?	☐ Yes ☒ No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Data is maintained for the life of the easement and for historical purposes to enable reports to Congress.
14.2	What are the procedures for purging the data at the end of the retention period?	N/A
14.3	Where are these procedures documented?	N/A
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	For the life of a grant, annual monitoring is used to ensure all requirements of the grant are being upheld.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☒ Yes ☐ No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	Processing of financial transactions by NFC.
17.2	Who is responsible for assuring the other agency properly uses the data?	NRCS and NFC each have the individual accountability to adhere to organizational and departmental policies and procedures and to establish agreements between stakeholders.
18	Is the data transmitted to another agency or an independent site?	☒ Yes ☐ No – If NO, go to question 19.

No.	Question	Response
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	NRCS and NFC each have the responsibility to identify and categorize the type of information processed and certify and accredit their applications (*CRM Common Desktop* and *FFIS*, respectively).
19	Is the system operated in more than one site?	☒ Yes ☐ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	Primary and cold failover *CRM Common Desktop* application systems will be operated in two different USDA Data Centers in an Active-Passive stance.

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	Only NRCS users and affiliates with a valid need to know are granted access. Appropriate separation of duties is enforced for critical transactions.
21	How will user access to the data be determined?	Access to the *CRM Common Desktop* application is limited to NRCS employees and affiliates who have been assigned areas of responsibility within the Easement programs (e.g., WRP and FRPP).
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No
22	How will user access to the data be restricted?	The *CRM Common Desktop* application will inherit Access Control from Active Directory and zRoles to implement roles-based access within the application.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No In order to prevent browsing and/or unauthorized access users are authenticated via active directory and authorized via zRoles. Additionally, the *CRM Common Desktop* application enforces role-based access and all users must be assigned to a specific role in order to use/access the application.
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☐ Yes ☒ No

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	NRCS
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	If incident response assistance is needed Customers and employees can contact the NRCS Security Response Team via the following numbers: • Lost and Stolen equipment NRCS 800 number (1-888-926-2373) and/or e-mail address (nrcs.security@usda.gov). • Personal Identifiable Incidents – 877-744-2968 (PII-2YOU) • NRCS/CD - (202) 757-8111 or (703) 200-3008
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 27. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	Consider the following: • Consolidation and linkage of files and systems • Derivation of data • Accelerated information processing and decision making • Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	The system will only implement the rules and procedures contained with the appropriate Programs (e.g., WRP, FRPP). These programs have processes in place to ensure equitable treatment of customers.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes ☐ No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	SCIMS IDs are used to retrieve data.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	Notice of Privacy Act System of Records by Owner, Operator or Producer Files (or Volunteer / Employee Files) USDA/NRCS-1. http://www.nrcs.usda.gov/about/foia/408_45.html
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	☐ Yes ☒ No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.
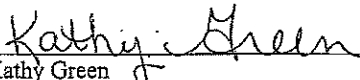
Privacy Impact Assessment Authorization

Memorandum

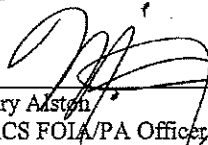I have carefully assessed the Privacy Impact Assessment for the

Natural Resources Conservation Service – *CRM Common Desktop*

(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.
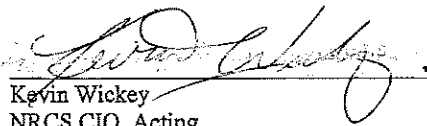
We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Kathy Green
NRCS ITC Development Branch Chief

10-21-09
Date

Mary Alston
NRCS FOIA/PA Officer

12-23-09
Date

Kevin Wickey
NRCS CIO, Acting

12-28-2009
Date